

UNITED STATES DISTRICT COURT
for the
Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)

Account jaybirdchest@gmail.com, stored at
premises owned, maintained, controlled, or
operated by Google, LLC, a company located at
1600 Amphitheatre Parkway, Mountain View,
California 94043

Case No. 20-MJ-749

APPLICATION FOR A SEARCH WARRANT

I, Barry Couch, Special Agent, FBI, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of New York (identify the person or describe property to be searched and give its location): **The account jaybirdchest@gmail.com, stored at premises owned, maintained, controlled, or operated by Google, LLC, a company located at 1600 Amphitheatre Parkway, Mountain View, California 94043, as further described in Attachment A.**


The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): **See Attachment B for the Evidence to be Seized, all of which are evidence, contraband, fruits, and instrumentalities of violations of Title 18 United States Code, Section 2252A(a)(5)(B), and all of which are more fully described in the application and affidavit filed in support of this warrant, the allegations of which are adopted and incorporated by reference as if fully set forth herein.**

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 2252A(a)(5)(B), and the application is based on these facts which are continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____), is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Barry Couch, Special Agent, F.B.I.
Printed name and title

Application submitted by email/pdf and attested to me and before me as true and accurate by telephone consistent with Fed.R.Crim.P. 4.1 and 41(d)(3).

Date: October 14, 2020


Judge's signature

City and state: Rochester, New York

Hon. Mark W. Pedersen, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

STATE OF NEW YORK)
COUNTY OF MONROE) SS:
CITY OF ROCHESTER)

I, BARRY W. COUCH, being duly sworn, depose and state:

1. I am a Special Agent with the Federal Bureau of Investigation and have been so for approximately eleven years. I am currently assigned to the Buffalo Division, Rochester, New York, Resident Agency. My duties involve investigating federal crimes including violations of Title 18, United States Code, Section 2252A.

2. This affidavit is made in support of an application for a warrant to search the contents of the Google account associated with the jaybirdchest@gmail.com email address (hereinafter the "SUBJECT ACCOUNT").

3. The information contained in this affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers, and the review of documents and records.

4. As is set forth in more detail below, there is probable cause to believe that evidence, contraband, fruits and instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) are located within the SUBJECT ACCOUNT.

5. Because this affidavit is being submitted for the limited purpose of establishing probable cause to secure a search warrant, I have not included every detail of the investigation. Rather, I have set forth only the facts that I believe are sufficient to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 2252A(a)(5)(B) is presently located in the SUBJECT ACCOUNT.

6. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part.

BACKGROUND OF INVESTIGATION

7. On or about December 14, 2011, Jason KOSCIELSKI plead guilty in the United States District Court for the Western District of New York (Case No. 10-CR-6237) to a 6-count Indictment charging him with Possession of Child Pornography (Counts 1 & 2), Receipt of Child Pornography (Counts 3 & 4), and Distribution of Child Pornography (Counts 5 & 6).

8. On or about January 24, 2013, the Hon Charles A. Siragusa sentenced KOSCIWLSKI to a term of imprisonment of 135 months to be followed by 30 years of supervised release. One of the conditions of supervised release that Judge Siragusa imposed was:

SPECIAL CONDITIONS OF SUPERVISION

The defendant must provide the U.S. Probation Office advance notification of any computer(s), automated service(s), or connected device(s) that will be used during the term of supervision. The U.S. Probation Office is authorized to install any application as necessary to surveil all activity on computer(s) or connected device(s) owned or operated by the defendant. The defendant may be required to pay the cost of monitoring services at the monthly rate provided by the U.S. Probation Office. The rate and payment schedule are subject to periodic adjustments by the U.S. Probation Office. The U.S. Probation Office shall be notified via electronic transmission of impermissible/suspicious activity or communications occurring on such computer or connected device, consistent with the computer monitoring policy in effect by the probation office. As triggered by impermissible/suspicious activity, the defendant shall consent to and cooperate with unannounced examinations of any computer equipment owned or used by the defendant. This examination shall include but is not limited to retrieval and copying of all data from the computer(s), connected device(s), storage media, and any internal or external peripherals, and may involve removal of such equipment for the purpose of conducting a more thorough inspection.

(Case No. 10-CR-6237, Dkt. 56, p. 4.)

9. On or about September 5, 2020, KOSCIELSKI was released from the Bureau of Prisons' custody and began his term of supervised release. KOSCIELSKI was to be supervised by the United States Probation Office ("USPO") in Rochester, New York.

10. To that end, on September 15, 2020, KOSCIELSKI met with United States Probation Officer ("PO") Jillian Trahms to review the terms of his supervision. During that meeting, KOSCIELSKI told PO Trahms that he was in possession of an unmonitored cell phone. PO Trahms immediately confiscated the cell phone for review and installation of monitoring software.

11. On the morning of September 16, 2020, United States Probation Officer Assistant ("POA") Troy Zeller reviewed the phone to confirm the device met specifications needed for the monitoring software to work and to verify there was no nefarious activity on the device prior to install, as per United States Probation Office computer monitoring procedures.

12. In the course of doing so, POA Zeller reviewed the internet browser history and observed several browser entries that appeared to be Russian internet sites that were viewed.

13. POA Zeller brought the device to Supervisory United States Probation Officer Roosevelt Smith, Jr., to staff the case. SUPV Smith observed the browser history and saw the same data that POA Zeller had observed. According to SUPV Smith, the search history included search term “boys, little, pee, and peeing.” SUPV Smith also observed several images following the search terms that depicted child-age boys with their genitals exposed either on the toilet or standing in several different environment settings. The browsing history included dates of activity as recent as September 15, 2020 (the same day KOSCIELSKI turned the phone over to PO Trahms).

14. SUPV Smith then reviewed the photo gallery application on the phone—which is also part of a standard review of the device and which, based on SUPV Smith’s knowledge and training, is used to store both images that are captured by the phone’s camera and images that are downloaded from texts and internet sites. In the photo section, SUPV Smith observed several pornographic images including images of an erect penis, cartoon pornography and several images of the defendant. In addition, in the folder marked deleted, within the same photo gallery app, SUPV Smith observed two videos that appeared to be children involved in sexual acts.

15. That day, I was contacted by SUPV Smith and asked to review the videos he found on the phone. I observed one video that showed two boys, approximately 14 years old, engaged in anal sex. I observed a second video that showed a boy, approximately 10 years old, fully naked, masturbating. Based upon my training and experience in the investigation of child pornography cases, these videos constitute child pornography, as defined by Title 18, United States Code, Section 2256(8).

16. Later on September 16, 2020, KOSCIELSKI was interviewed by SUPV Smith. During that interview, KOSCIELSKI stated that he purchased the phone new from T-Mobile approximately two months earlier and that it was his phone. When told two videos of concern were located in his phone's photo trash, KOSCIELSKI stated he had received those videos, along with others, from a "friend." When asked if he thought the videos were appropriate for him to have, he responded, "the kids in the videos were young."

17. On or about September 16, 2020, PO Trahms filed a Petition for Warrant or Summons for Offender Under Supervision, which charged KOSCIELSKI with violating the conditions of his supervision by (a) committing another federal, state, or local crime and (b) possessing and downloading child pornography (the "Violation Petition"). Pursuant to the Violation Petition and a corresponding warrant issued by Judge Siragusa, KOSCIELSKI was taken into custody that same day. On or about September 17, 2020, KOSCIELSKI was arraigned on the Violation Petition. The government moved to detain KOSCIELSKI and he remains in custody pending further proceedings.

18. KOSCIELSKI is represented by AFPD Wedade W. Abdallah. On September 17, 2020, Ms. Abdallah sent an email to AUSA Meghan K. McGuire stating as follows: "Jillian [Trahms, PO] mentioned that the FBI will be conducting a search of Mr. Koscielski's phone. Please note, Mr. Koscielski is not consenting to the search and seizure of his property by the FBI or any other law enforcement agency."

19. On September 23, 2020, I obtained a federal search warrant to search the contents of the phone. On September 24, 2020, I executed the search warrant. In my search

of the phone's contents, I observed what appeared to be the same things SUPV Smith had observed, including the same two videos of child pornography described in paragraphs 14 and 15, above.

20. Those videos were located in the "Trash" section of the Google Photos application on the phone. Under the Google application on the phone, I observed that KOSCIELSKI's Google account was jaybirdchest@gmail.com.

21. On or about September 29, 2020, I submitted a preservation request to Google for the SUBJECT ACCOUNT. As a result, the contents of the SUBJECT ACCOUNT will be preserved for at least 90 days.

TRAINING AND EXPERIENCE

22. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the possession of child pornography:

- a. Those who possess child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Those who possess child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videos, books, slides and/or drawings or other visual media. Such individuals often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of

children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual act.

- c. Those who possess child pornography often possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, videos, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location such as an online account. These individuals sometimes retain pictures, films, videos, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, and child erotica for many years.
- d. Likewise, those who possess child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer, cell phone, other digital device, or online account. These collections are often maintained for several years and are kept close by, to enable the collector to view the collection, which is valued highly. In many cases, the individual may try to hide the collection or may use a computer, such as a laptop, that can easily be transported from one location to another, in order to keep his collection private and not make it known to other individuals he or she may be residing with.
- e. Those who possess child pornography also may correspond with and/or meet others to share information and materials; often maintain correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Those who possess child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Files of child pornography stored in online accounts can sometimes be viewed by the online account company even after having been deleted.

BACKGROUND REGARDING GOOGLE

23. Google was the service provider for the email address referenced within this affidavit. Based on my training and experience and my conversations with other law enforcement officers, I have learned the following about Google:

- a. Google is a company that provides a variety of online services, including electronic mail ("email") access to the public. A Google subscriber can also store with Google files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.
- b. Google is considered an electronic communications service ("ECS") provider because it provides its users access to electronic communications service as defined in Title 18, United States Code, Section 2510(15). Internet users sign-up for a subscription for these electronic communication services by registering on the Internet with Google. Google requests subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information. However, Google does not verify the information provided. As part of its services, Google also provides its subscribers with the ability to set up email accounts.
- c. Google maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts.
- d. Subscribers to Google may access their accounts on servers maintained or owned by Google from any computer connected to the Internet located anywhere in the world.
- e. Emails and image files stored on a Google server by a subscriber may not necessarily also be located in the subscriber's home computer. The subscriber may store emails and/or other files on the Google server for which there is insufficient storage space in the subscriber's own computer or which the subscriber does not wish to maintain in his or her own computer. A search of the subscriber's home, business, or laptop computer will therefore not necessarily uncover files the subscriber has stored on the Google servers.

CONCLUSION

24. Based upon the forgoing, the undersigned respectfully submits that there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(5)(B), as specifically described in Attachment B to this application, are presently located within the SUBJECT ACCOUNT. The undersigned therefore respectfully requests that the attached warrant be issued authorizing a

search and seizure for the items listed in Attachment B within the SUBJECT ACCOUNT, more particularly described in Attachment A to this application.



BARRY W. COUCH
Special Agent
Federal Bureau of Investigation

Affidavit submitted electronically by email in .pdf format. Oath administered, and contents and signature, attested to me as true and accurate telephonically pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on this 14th day of October, 2020.



HON. MARK W. PEDERSEN
United States Magistrate Judge

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant is directed to Google, LLC (the “Service Provider”), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, and applies to all content and other information within the Service Provider’s possession, custody, or control associated with the account jaybirdchest@gmail.com (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it *via* email or another appropriate manner to the Service Provider. The Service Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Attachment B, Section I. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Attachment B, Section II.

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

I. Information to be disclosed by Google (the “Service Provider”)

To the extent within the Service Provider’s possession, custody, or control, regardless of whether such information is located within or outside of the United States, and including any communications, records, files, logs, or information that has been deleted but is still available to the Service Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on or about September 29, 2020, the Service Provider is required to disclose the following information to the government for the Subject Account, as defined in Attachment A:

a. The contents of all text messages, voicemails, recorded calls, emails, and chat messages associated with the account, including stored or preserved copies of chat logs, emails sent to and from the account, draft communications, the source and destination addresses associated with each communication, the date and time at which each communication was sent, and the size and length of each communication;

b. All records or other information regarding the identification of the account subscriber and/or user(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, login IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All device information associated with the account to include, but not limited by, IMEI/MEID, serial number, SIM operator, cell operator, and model number;

d. All location history associated with the account. All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates, the dates and times of all location recordings, and origin of how the location recordings were obtained and estimated radius;

e. Web search history, including, but not limited to, mobile and desktop browser searches;

f. The types of service utilized;

g. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

h. All records pertaining to communications between the Service Provider and any person regarding the account, including contacts with support services and records of actions taken.

i. Voice and/or audio activity captures;

j. Google Map location saved and/or frequent locations, favorite and/or starred locations including, but not limited to, searches conducted using the Google Map and/or Maze services;

k. Communication including, but not limited to, audio, video, text message and/or chat delivered through the Google, Inc. service known as Google Hangouts;

l. Posts, status updates, and/or any other information including photographs and/or video for the Google, Inc. service known as Google+;

m. Photographs and/or videos that are contained and/or were uploaded in the Google, Inc. services known as Google Photos, Picasa web albums, Google+, or any other Google, Inc. service designed to store video, photographs, and/or data, including the metadata for each file, including those that have been deleted if still available;

n. Electronic files, folders, media, and/or data uploaded and/or contained on the Google, Inc. service known as Google Drive;

o. Historical account information, including call forwarding numbers and account backup telephone number; subscriber registration information, sign-up IP address and associated time stamp, telephone connection records, billing information, stored text message content, stored voicemail content, any and all apps installed using referenced email, Google Play Store transactions, call records, and IP log information.

II. Information to be Searched for and Seized by the Government

Any and all records or information, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information that contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(5) (Possession of Child Pornography), including, but not limited to information pertaining to:

a. The contents of any communications that relate to the possession or accessing with intent to view of child pornography, as defined by 18 U.S.C. § 2256(8);

b. Records relating to who created, used, or communicated with the Subject Account;

c. Records, including but not limited to video files, audio files, images, stored messages, recordings, books, documents, and cached web pages relating to the possession or

accessing with intent to view of child pornography;

d. All visual depictions, including still images, videos, films or other recordings of child pornography, as defined in Title 18, United States Code, Section 2256(8), and any mechanism used for the receipt or storage of the same; and

e. Web search history, including, but not limited to, mobile and desktop browser searches, relating to the possession, accessing with intent to view, or attempting to possess or access with intent to view of child pornography, as defined by 18 U.S.C. § 2256(8);

f. Records relating to any attempt(s) to clear or delete the web search history, cookies, or other historical information related to the Subject Account; and

g. Any other identifying information associated with the user of the account (financial information, employment information, patterns of behavior, etc.).